1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

011113820 **Image available**
WPI Acc No: 1997-091745/ **199709**
XRPX Acc No: N97-075652
Computer network system for e.g. security processing, access management - uses data transceiver of each connected data processor in sending and receiving formed description data as user identifier through communication network
Patent Assignee: TOSHIBA KK (TOKE)
Inventor: ITSUMI K; NUKUI H; UCHIDA S
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 8329010	A	19961213	JP 9659806	A	19960315	199709	B
US 5887140	A	19990323	US 96622608	A	19960326	199919	

Priority Applications (No Type Date): JP 9568185 A 19950327
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 8329010	A		23	G06F-015/00	
US 5887140	A			G06K-009/00	

Abstract (Basic): JP 8329010 A

The system (10) has several data processors (11-1-11-3) connected through a communication network (12). Each data processor has a measuring unit that measures the physical description of a user.

A data generator forms a description data based on the measured physical description. A data transceiver sends and receives the formed description data as a user identifier through the communication network.

ADVANTAGE - Reliably maintains security. Determines access right based on access demand of user at high speed. Reduces user load since reliable authentication processing is performed through easy operation. Eliminates complex password input operation in access processing. Ensures high-speed collation processing. Increases capacity of file system ten times higher than conventional system.

Dwg.1/15
Title Terms: COMPUTER; NETWORK; SYSTEM; SECURE; PROCESS; ACCESS; MANAGEMENT ; DATA; TRANSCEIVER; CONNECT; DATA; PROCESSOR; SEND; RECEIVE; FORMING; DESCRIBE; DATA; USER; IDENTIFY; THROUGH; COMMUNICATE; NETWORK
Derwent Class: T01
International Patent Class (Main): G06F-015/00; G06K-009/00
International Patent Class (Additional): G06F-013/00; G06T-007/00
File Segment: EPI

1/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

05373510 **Image available**
COMPUTER NETWORK SYSTEM, ITS ACCESS ADMINISTRATING METHOD, AND INDIVIDUAL AUTHORIZATION DEVICE USED FOR SAME

PUB. NO.: 08-329010 [**JP 8329010** A]
PUBLISHED: December 13, 1996 (19961213)
INVENTOR(s): HENMI KAZUHIRO
UCHIDA SATOSHI
NUKUI HARUMI
APPLICANT(s): TOSHIBA CORP [000307] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-059806 [JP 9659806]
FILED: March 15, 1996 (19960315)

INTL CLASS: [6] G06F-015/00; G06F-013/00; G06T-007/00
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 45.2 (INFORMATION PROCESSING -- Memory Units); 45.9 (INFORMATION PROCESSING -- Other)
JAPIO KEYWORD: R124 (CHEMISTRY -- Epoxy Resins)

ABSTRACT

PURPOSE: To perform a processing for deciding whether or not a user has access right speedily at a user's access request by using physical body feature data and to securely maintain secrecy protection.

CONSTITUTION: At the access request, the physical body features of the user are measured by feature measurement units 14-1, 14-2, and 14-3, and further processed by data degeneration units 13-1, 13-2, and 13-3 as feature data having linear projection, etc., degenerated. Computer systems 11-1 and 11-2 send the feature data to a collation server 15 through a communication network 12. The collation server 15 performs a collation process according to feature data previously stored in a file system 16. It is judged from the collation result whether or not the user has the access right, and the access allowed/disallowed state is sent to computer systems 11-1 and 11-2.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－329010

(43)公開日　平成８年(1996)12月13日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０	9364－5L	Ｇ０６Ｆ	15/00	３３０Ｆ
	13/00	３５５	7368－5E		13/00	３５５
Ｇ０６Ｔ	7/00				15/62	４６０

審査請求　未請求　請求項の数14　ＯＬ　（全 23 頁）

(21)出願番号　特願平8－59806

(22)出願日　平成８年(1996)３月15日

(31)優先権主張番号　特願平7－68185

(32)優先日　平７(1995)３月27日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　逸見　和弘
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　内田　智
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(72)発明者　貫井　春美
東京都府中市東芝町１番地　株式会社東芝府中工場内

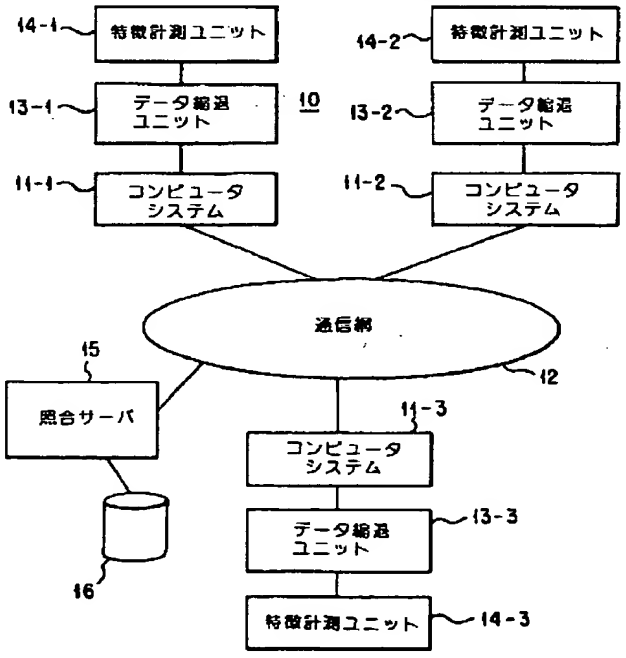
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　コンピュータネットワークシステム、このコンピュータネットワークシステムにおけるアクセス管理方法、及びこのコンピュータネットワークシステムにおいて使用される個人認証装置

(57)【要約】

【課題】　コンピュータネットワークシステムにおいて、身体的特徴データを用い、使用者からのアクセス要求に応じてアクセス権の有無を判別する処理を高速に行い、且つ、確実に機密保護を維持する。

【解決手段】　アクセス要求に応じ、使用者の身体的特徴が特徴計測ユニット１４により計測され、更に、データ縮退ユニット１３において、一次元射影等の縮退された特徴データとして処理される。コンピュータシステム１１は、通信網１２を介してこの特徴データを照合サーバ１５に送出する。照合サーバ１５は、ファイルシステム１６に予め登録されている特徴データに従って照合処理を行う。この照合結果に応じて、使用者のアクセス権の有無が判断され、アクセス許可／不許可の旨がコンピュータシステム１１に送られる。



1

【特許請求の範囲】

【請求項１】　複数のデータ処理手段と前記複数のデータ処理手段を相互接続する通信手段とにより構成されるコンピュータネットワークシステムにおいて、

前記複数のデータ処理手段はそれぞれ、

使用者の身体的特徴を測定する測定手段と、

測定された身体的特徴を縮退して特徴データを生成する生成手段と、

前記特徴データを使用者識別子として前記通信手段を介して送受するデータ送受手段とを具備することを特徴とするコンピュータネットワークシステム。

【請求項２】　前記複数のデータ処理手段は、アクセス要求に応じて前記使用者識別子を送出し、

前記通信手段に接続され、前記通信手段を介して受け取った使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する照合手段を具備することを特徴とする請求項１記載のコンピュータネットワークシステム。

【請求項３】　前記コンピュータネットワークシステムは、任意のデータを予め設定された順序で前記複数のデータ処理手段に送出するワークフローシステムであって、

前記複数のデータ処理手段はそれぞれ、前記使用者識別子が予め登録されている使用者識別子と一致した場合のみ、前記任意のデータの受信に応じて承認・非承認の判定を受け付ける手段を有することを特徴とする請求項１記載のコンピュータネットワークシステム。

【請求項４】　前記コンピュータネットワークシステムは、任意のデータを予め定められた順序で前記複数のデータ処理手段に送出するワークフローシステムであって、

前記通信手段に接続され、前記通信手段を介して受け取った使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する照合手段を具備し、

前記複数のデータ処理手段はそれぞれ、アクセス要求に応じて前記使用者識別子を送出し、前記照合手段がアクセス要求可と判定した場合のみ、前記データの受信に応じた承認・非承認の判定を受け付ける手段を有することを特徴とする請求項１記載のコンピュータネットワークシステム。

【請求項５】　前記複数のデータ処理手段はそれぞれ、アクセス要求に応じ、前記使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する手段を有することを特徴とする請求項１記載のコンピュータネットワークシステム。

【請求項６】　前記複数のデータ処理手段はそれぞれ、他のデータ処理手段からのアクセス要求に応じ、このアクセス要求元のデータ処理手段から使用者識別子を受取り、前記予め登録された使用者識別子と照合してアクセス要求の可否を判定する手段を有することを特徴とする請求項５記載のコンピュータネットワークシステム。

2

【請求項７】　前記生成された特徴データは、一次元射影であることを特徴とする請求項１記載のコンピュータネットワークシステム。

【請求項８】　前記測定手段は、線状電極アレイを有し、

前記生成手段は、前記線状電極アレイに前記使用者の指が載置された際、隣接した各線状電極の抵抗値の分布を検出することを特徴とする請求項１記載のコンピュータネットワークシステム。

【請求項９】　前記照合手段は、前記使用者識別子と、前記予め登録された使用者識別子との位置合わせを行い、位置合せされた前記使用者識別子と前記予め登録された使用者識別子との相違度を算出し、算出された相違度と予め設定されたしきい値とを比較してアクセス可否を判定することを特徴とする請求項２記載のコンピュータネットワークシステム。

【請求項１０】　複数のデータ処理手段と、この複数のデータ処理手段を相互接続する通信手段とを有するネットワークシステムにおけるアクセス管理方法であって、

アクセス要求に応じ、使用者の身体的特徴を測定するステップと、

測定された身体的特徴を縮退して特徴データを生成するステップと、

前記特徴データを使用者識別子として前記通信手段を介して送受するステップとを具備することを特徴とするアクセス管理方法。

【請求項１１】　前記通信手段を介して送受される前記使用者識別子を、予め登録された使用者識別子と照合するステップと、

前記照合ステップの照合結果に従って、アクセス要求の可否を判定するステップとを具備することを特徴とする請求項１０記載のアクセス管理方法。

【請求項１２】　前記生成ステップにより生成された特徴データは、一次元射影であることを特徴とする請求項１０記載のアクセス管理方法。

【請求項１３】　前記照合ステップは、

前記使用者識別子と、前記予め登録された使用者識別子との位置合わせを行うステップと、

位置合せされた前記使用者識別子と前記予め登録された使用者識別子との相違度を算出するステップと、

算出された相違度と予め設定されたしきい値とを比較するステップとを有することを特徴とする請求項１１記載のアクセス管理方法。

【請求項１４】　複数のデータ処理装置が相互接続されたネットワークシステムにおける個人認証装置であって、

基板上に一次元に配列された線状電極アレイのアレイ方向に沿って被認証者の指が接触することによる前記線状

電極アレイの隣接電極間の抵抗値の分布に基づいて特徴データを出力する特徴抽出手段と、
前記特徴抽出手段から出力される特徴データと予め登録されている特徴データとの位置合わせ処理を行う位置合わせ手段と、
この位置合せ手段により位置合わせされた前記特徴データと前記登録された特徴データとの相違度を算出する相違度計算手段と、
相違度計算手段により算出された相違度と予め設定されたしきい値とを比較して前記被認証者の認証を判定する判定手段とを具備することを特徴とする個人認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、複数のコンピュータシステムが通信網を介して相互に接続されることにより構成されるコンピュータネットワークシステム、このコンピュータネットワークシステムにおけるアクセス管理方法、及びこのコンピュータネットワークシステムにおいて使用される個人認証装置に関し、特に、使用者の身体的特徴データを用いてセキュリティ処理を行うコンピュータネットワークシステム、このコンピュータネットワークシステムにおけるアクセス管理方法、及びこのコンピュータネットワークシステムにおいて使用される個人認証装置に関する。

【０００２】

【従来の技術】複数のコンピュータ端末（システム）を通信網により相互に接続したコンピュータネットワークシステムでは機密保護のため、ネットワークシステムへのアクセス要求に応じて、使用者を識別してアクセス権の有無を判定する処理、即ちアクセスの許可判定処理を行う必要がある。

【０００３】使用者を識別する方法としては、使用者識別子としてパスワードをコンピュータ端末のキーボードから入力する方法が最も一般的に用いられている。しかし、この方法ではキーボードから入力されるパスワードのみが使用者識別の判定基準であるため、使用登録者以外でもパスワードを知りさえすればネットワークにアクセスでき、不正なアクセスを完全に防止することはできない。

【０００４】従って、セキュリティを向上させるためにパスワードを複雑にしたり、ネットワーク内の各コンピュータシステムから他のコンピュータシステムにアクセスする際には個別に専用パスワードを設定する等の対策が施されている。しかし、この方法では使用者が複雑なパスワードを複数種類記憶する必要があり、更にパスワードの入力操作も非常に手間がかかるため、使用者の負担が大きい。

【０００５】

【発明が解決しようとする課題】上述したように、コンピュータネットワークシステムにおいて、パスワードを用いてネットワークシステムまたはコンピュータシステムにアクセスを行う従来の方式では、完全な機密保護が困難であり、かつ使用者の操作が煩雑であるという問題点がある。

【０００６】この発明は上述した実情に鑑みてなされたものであり、身体的特徴データを用いることにより、使用者からのアクセス要求に応じてアクセス権の有無を判別する処理を高速に行うことができ、且つ、確実に機密保護を維持することが可能なコンピュータネットワークシステムを提供することを目的とする。

【０００７】又、この発明は、コンピュータネットワークシステムにおいて、身体的特徴データを用いることにより、使用者からのアクセス要求に応じてアクセス権の有無を判別する処理を高速に行うことができ、且つ、確実に機密保護を維持することが可能なアクセス管理方法を提供することを目的とする。

【０００８】又、この発明は、容易な操作で確実な認証処理を行い、使用者の負担を軽減することができる、コンピュータネットワークシステムにおいて使用される個人認証装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】この発明に係るコンピュータネットワークシステムは、複数のデータ処理手段と前記複数のデータ処理手段を相互接続する通信手段とにより構成されるコンピュータネットワークシステムであって、前記複数のデータ処理手段はそれぞれ、使用者の身体的特徴を測定する測定手段と、測定された身体的特徴を縮退して特徴データを生成する生成手段と、前記特徴データを使用者識別子として前記通信手段を介して送受するデータ送受手段とを具備することを特徴とする。

【００１０】前記コンピュータネットワークシステムにおいて、前記複数のデータ処理手段は、アクセス要求に応じて前記使用者識別子を送出し、前記通信手段に接続され、前記通信手段を介して受け取った使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する照合手段を具備することを特徴とする。

【００１１】この発明に係るアクセス管理方法は、複数のデータ処理手段と、この複数のデータ処理手段を相互接続する通信手段とを有するネットワークシステムにおけるアクセス管理方法であって、アクセス要求に応じ、使用者の身体的特徴を測定するステップと、測定された身体的特徴を縮退して特徴データを生成するステップと、前記特徴データを使用者識別子として前記通信手段を介して送受するステップとを具備することを特徴とする。

【００１２】前記アクセス管理方法は更に、前記通信手段を介して送受される前記使用者識別子を、予め登録された使用者識別子と照合するステップと、前記照合ステップの照合結果に従って、アクセス要求の可否を判定す

るステップとを具備することを特徴とする。

【００１３】以上のコンピュータネットワークシステム、またはアクセス管理方法においては、人間の身体的特徴、例えば指の特徴を抽出して得られる特徴データは指紋に依存するものであり、各個人に固有のものである。従って、この特徴データを使用者識別子として用いてネットワークシステムに対するアクセス権の有無を判定すれば、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護ができ、かつ煩雑な入力操作を必要としないので、アクセス操作における使用者の負担が軽減される。

【００１４】又、このシステムで用いられる特徴データは縮退されたデータであり、一般的な指紋画像を用いるものに比べて、データ量が約１０分の１となり、ネットワーク上での通信網を介した転送や、照合サーバでの照合等の処理を高速で行うことができる。同様に、照合処理に必要とされるファイルシステムの容量も従来の約１０分の１でよい。

【００１５】又、このようなコンピュータネットワークシステムにおいて、一度ネットワークへのアクセスが認められた場合、指の特徴データをあるコンピュータシステムから他のコンピュータシステムにアクセスする際の使用者識別子として使用することにより、従来のように他のコンピュータシステムにアクセスする際に必要としていた煩わしい手順が簡略化される。

【００１６】又、前記複数のデータ処理手段はそれぞれ、アクセス要求に応じ、前記使用者識別子を、予め登録された使用者識別子と照合し、アクセス要求の可否を判定する手段を有する構成であってもよい。更に、前記複数のデータ処理手段はそれぞれ、他のデータ処理手段からのアクセス要求に応じ、このアクセス要求元のデータ処理手段から使用者識別子を受取り、前記予め登録された使用者識別子と照合してアクセス要求の可否を判定する手段を有する構成であってもよい。

【００１７】前記生成された特徴データは、一次元射影等の縮退されたデータである。又、前記測定手段は、線状電極アレイを有し、前記生成手段は、前記線状電極アレイに前記使用者の指が載置された際、隣接した各線状電極の抵抗値の分布を検出する構成であってもよい。

【００１８】前記照合手段または照合ステップは、前記使用者識別子と、前記予め登録された使用者識別子との位置合わせを行い、位置合せされた前記使用者識別子と前記予め登録された使用者識別子との相違度を算出し、算出された相違度と予め設定されたしきい値とを比較してアクセス可否を判定することが好ましい。

【００１９】又、前記発明に係るコンピュータネットワークシステムは、任意のデータを予め設定された順序で前記複数のデータ処理手段に送出するワークフローシステムであって、前記複数のデータ処理手段はそれぞれ、前記使用者識別子が予め登録されている使用者識別子と一致した場合のみ、前記任意のデータの受信に応じて承認・非承認の判定を受け付ける手段を有することを特徴とする。

【００２０】従って、コンピュータネットワークシステム上に設定された一連の仕事の流れを運用するワークフローシステムにおいて、予め設定した条件によって承認・非承認の判定を行う判定処理の際に、予め登録してある指の特徴データと判定時に入力された指の特徴データが一致した場合のみに判定処理を行うことができるようにすることで、操作が容易でかつ確実な電子承認が可能となる。

【００２１】前述した測定部及び生成部は、線状電極アレイのアレイ方向に沿って使用者の指が接触することによる隣接電極間の抵抗値の分布から指の特徴を抽出して、指の長手方向に沿った一次元の特徴抽出データを出力する。従って、指紋を２次元の画像として検出する指紋センサに比較して特徴データのデータ量が著しく少ないため、コンピュータネットワークシステム上での転送や登録されている特徴データとの照合処理を高速に行うことができ、従って迅速に個人認証を行うことが可能となる。

【００２２】この発明に係る個人認証装置は、複数のデータ処理装置が相互接続されたネットワークシステムにおける個人認証装置であって、基板上に一次元に配列された線状電極アレイのアレイ方向に沿って被認証者の指が接触することによる前記線状電極アレイの隣接電極間の抵抗値の分布に基づいて特徴データを出力する特徴抽出手段と、前記特徴抽出手段から出力される特徴データと予め登録されている特徴データとの位置合わせ処理を行う位置合わせ手段と、この位置合せ手段により位置合わせされた前記特徴データと前記登録された特徴データとの相違度を算出する相違度計算手段と、相違度計算手段により算出された相違度と予め設定されたしきい値とを比較して前記被認証者の認証を判定する判定手段とを具備することを特徴とする。

【００２３】これにより、指紋を２次元の画像として検出する指紋センサに比較して特徴データのデータ量が著しく少ないため、コンピュータネットワークシステム上での転送や登録されている特徴データとの照合処理を高速に行って、迅速な個人認証が可能であると共に、被認証者の指と線状電極アレイの相対位置が登録時と多少異なっていても、位置合わせ処理を行うことにより、抽出された特徴データと登録されている特徴データとの比較照合を正確に行うことができる。

【００２４】

【発明の実施の形態】以下、この発明に係る第１の実施の形態～第４の実施の形態を図面を参照して説明する。図１は、この発明の第１の実施の形態に係るコンピュータネットワークシステム１０の概略構成を示すブロック図である。同図に示されるように、複数のコンピュータ

システム１１（１１－１～１１－３）が通信網１２を介して相互に接続されている。各コンピュータシステム１１にはぞれぞれデータ縮退ユニット１３（１３－１～１３－３）を介し、使用者の身体的特徴（特徴データ）を計測する特徴計測ユニット１４（１４－１～１４－３）がそれぞれ接続されている。このデータ縮退ユニット１３及び特徴計測ユニット１４により使用者の身体的特徴が電気信号として抽出される。

【００２５】尚、この実施の形態では、特徴計測ユニット１４は、使用者の身体的特徴として後述するように使用者の指の指紋情報を測定する。身体的特徴とは、人間の身体に係る情報であって、各個人に固有の特徴を意味する。又、図１に示されるコンピュータネットワークシステム１０には、３つのコンピュータシステム１１が接続されているが、接続されるコンピュータシステムの数はこれに限定されない。

【００２６】通信網１２には、更に、各特徴計測ユニット１４により測定された特徴データに基づいてコンピュータネットワークシステムに対する使用者のアクセス権の有無を識別する照合サーバ１５が接続されている。この照合サーバ１５はコンピュータシステム１１から通信網１２を介して送られる縮退された特徴データ（以降、抽出特徴データと称する）と、このコンピュータネットワークシステムにおいて予め登録されている指の特徴データ（以降、登録特徴データと称する）とを照合し、使用者つまり被認証者がアクセス権を有するか否かを判定する。

【００２７】尚、登録特徴データは、この実施の形態ではファイルシステム１６に保持される。次に、前記図１に示されるデータ縮退ユニット１３及び特徴計測ユニット１４による身体的特徴の抽出処理を図２～図４を参照して説明する。特徴計測ユニット１４は、前述したように、識別対象である使用者の指の指紋情報を測定する。データ縮退ユニット１３は、特徴計測ユニット１４により計測された指紋情報を、抽出特徴データとして電気信号で算出する。この際、フィルタリング処理やアナログ／デジタル変換処理等を施す。このデータ縮退ユニット１３により求められた抽出特徴データは、例えば、指の表面画像を示すデータに比べて情報量が少ない、一次元射影等の縮退されたデータである。

【００２８】ここで、縮退データについて説明する。通常、指紋画像、顔画像、声、目の網膜等の身体的特徴を測定した時の測定データには、複数の特徴が含まれている。例えば、二次画像は複数の一次画像で構成されている。この複数の特徴の内、幾つかの特徴を演算処理により消去、または他の特徴と等価な値に変換することにより、データ全体の情報量を減ずることを縮退、または縮退処理とし、縮退データとは、このような処理が施されたデータを示す。

【００２９】先の演算処理には、専用回路によるデータ処理や計算、または、専用のデバイス（電極アレイや光学式演算装置等）による測定が該当する。従って、フィルタリング処理もデータの縮退処理とみなすことができる。

【００３０】このような縮退処理には、一次元射影（三次元画像の場合は二次元射影）、輪郭の抽出、ベクトル（ベクトルの動き）抽出、フーリエ変換、特徴抽出、スムージング等がある。

【００３１】ここで、特徴計測ユニット１４及びデータ縮退ユニット１３とが一体となった特徴計測及びデータ縮退ユニットの構成例を図２（ａ），（ｂ）に示す。図２（ａ）は、前記一体とされた構成であるユニット上に識別対象である指が載置された場合の側面を示し、図２（ｂ）は、後述する線状電極と、識別対象である指の指紋との載置関係を示す。

【００３２】絶縁性の基板１４１の表面に線状電極アレイ１４２が形成されている。この線状電極アレイ１４２は、複数の線状電極を一次元のアレイ状に配列したものである。基板１４１の材料としては、例えばガラスエポキシその他のプリント基板材料、セラミック板、あるいは絶縁被覆を施した金属薄板などが用いられる。線状電極アレイ１４２の電極材料としては、例えばＣｕ薄膜、Ａｕ薄膜、Ｎｉメッキ膜、Ｐｔ薄膜あるいはＰｄ薄膜のような、人体の皮膚から出る汗等の体液に侵されにくい導電性材料が用いられる。

【００３３】又、この電極材料としては、測定対象が比較的高抵抗であるために絶縁体以外の材料であればどのような材料でも適用可能であり、例えばＩＴＯ（酸化インジウム・スズ）等の酸化物膜でもよい。電極の形成方法に関しても特に制限はなく、メッキ・蒸着等通常の方法はいずれも適用することができる。

【００３４】線状電極アレイ１４２には使用者の指が接触されるので、電極間隔は数百μｍ程度の指紋ピッチ、即ち指紋を構成する凹凸ピッチ（約０．５ｍｍ）より細かいピッチとし、例えば０．１ｍｍ程度とする。また、線状電極アレイ１４２のアレイ方向の長さ（アレイ長）は、指の先端から第二関節を完全に含む長さとする。電極間隔は一定なので、アレイ長は電極数によって調整することができる。

【００３５】線状電極アレイ１４２を構成する各々の電極には、引き出し端子１４４が接続されている。特徴測定時には、図２（ａ），（ｂ）に示されるように、指１４３を線状電極アレイ１４２のアレイ方向に沿って、即ち電極の個々の長手方向に直交するように押し付ける。

【００３６】一体化されたデータ縮退ユニット１３及び特徴計測ユニット１４の画回路を図３に示す。特徴計測及びデータ縮退ユニットは、前記引き出し端子１４４に接続されているスイッチ回路１４５、基準抵抗Ｒref 、及び低電圧源Ｖｏ を有し、前記図２（ａ），（ｂ）に示される線状電極アレイ１４２（図３では、ｎ本の電極１

４２－１～１４２－ｎとして示している）上に指を押し付けたときの隣接する電極間の抵抗値を指の長さ方向に順次読み取る。

【００３７】通常、人間の指の表面は、汗口の配列に従って皮膚が隆起して指紋を形成しており、この汗口からは、常時汗が自然放散している。即ち、指紋凸部からは常にＮａやＣｌを微量に含む水分の放散がある。従って、線状電極アレイ１４２上に指が押し付けられると、指紋凸部の汗口から放散された水分（発汗）は、指紋凸部直下の線状電極に到達する。この時、水分が到達した電極間では、水分に依存するイオンにより電気抵抗が低下する。ゆえに、指紋の凸部に対応した部分のみがそれ以外の部分に比べて低抵抗の状態となる。

【００３８】このような発汗に応じた低抵抗状態の他にも、状電極アレイ１４２に識別対象となる使用者の指が押し付けられると、隣接する２つの電極１４２ｉ，１４２ｉ＋１（ｉ＝１，２，…，ｎ）間のスペースに指紋を形成する凸部が入り込む形となる。この場合、隣接する２つの電極１４２ｉ，１４２ｉ＋１間の抵抗値Ｒｉは、その電極間スペースに入り込む指の凸部の量に応じても変化することになる。つまり、電極間スペースに入り込む凸部の量が多ければ、それだけ抵抗値Ｒｉは低くなる。

【００３９】電極１４２－１～１４２－ｎには、引き出し端子１４４を介してスイッチ回路１４５が接続されている。スイッチ回路１４５は、アナログスイッチ、さらに具体的にはアナログマルチプレクサＩＣ(integrated circuit)を用いて構成してもよい。スイッチ回路１４５は、隣接する２つの電極１４２ｉ，１４２ｉ＋１を基準抵抗Ｒref を介して定電圧源Ｖo に接続する。

【００４０】例えば、図３の状態では破線で示されるように、電極１４２－１と１４２－２が基準抵抗Ｒref を介して定電圧源Ｖo に接続されている。基準抵抗Ｖref の両端の電位差Ｖｉは、次式で与えられる。

【００４１】Ｖｉ＝Ｒref ・Ｖo ／（Ｒref ＋Ｒｉ）

スイッチ回路１４５により、この電位差Ｖｉを検出すべき隣接する２つの電極の組み合わせを１４２－１と１４２－２，１４２－２と１４２－３，…１４２－ｎ-1と１４２－ｎと順次切り替えて、電位差Ｖｉを指の長さ方向に順次読み取る。このようにして読み取られる電位差Ｖｉを時系列にプロットすると図４に示すようになり、指の長手方向への多値射影と等価なパターンが得られる。なお、図４で横軸は隣接する２つの電極の位置を示し、縦軸は電位差Ｖｉを示している。

【００４２】前述したよ処理により得られた信号は、特徴計測及びデータ縮退ユニットにおいて更に、フィルタリングおよびアナログーディジタル変換が行われる。ここで、データ縮退ユニット１３から出力されるデータは、例えば、電極間の検出分解能を８ビットとした場合には約１００バイト程度のデータ量となる。このデータを示す信号パターンをＡ（ｉ）とする。

【００４３】又、ここで求められた特徴データは、一般的な指紋画像を用いるものに比べて、大きさ（データ量）が約一桁も小さいため、図１のコンピュータネットワーク上での通信網１２を介しての転送や、照合サーバ１５での照合等の処理を高速で行うことができるという大きな利点を有している。

【００４４】例えば、人間の指の指紋画像では、指紋画像は圧縮処理が施された場合であっても、通常、１Ｋバイト程度のデータ量となる。本願では、前述したように人間の身体的特徴を縮退することにより、指紋情報であれば、約１００バイトで、指紋画像の約１０分の１のデータ量でよい。同様に、照合処理に必要とされるファイルシステム１６の容量も従来の約１０分の１でよい。

【００４５】次に、照合サーバ１５について説明する。図５は照合サーバ１５の構成を示す機能ブロック図である。照合サーバ１５は、位置合わせ処理部１５１、相違度計算部１５２および比較部１５３により構成される。

【００４６】位置合わせ処理部１５１は、特徴計測ユニット１４及びデータ縮退ユニット１３により抽出された抽出特徴データを表わす信号パターンＡ（ｉ）と、ファイルシステム１６から読み出された登録特徴データを表わす登録信号パターンＡｄ（ｉ）との位置合わせを行う。

【００４７】ファイルシステム１６に保持されている登録特徴データは、特徴計測ユニット１４において、指を線状電極アレイ１４２上にある一定の状態で置いたときに得られた特徴データである。しかし、照合処理を行うために計測をする場合、即ち、抽出特徴データを得るとき、特徴計測ユニット１４上で使用者が指を置く状態は、登録特徴データを得たときと同じとは限らない。即ち、指を載置する位置が微妙に異なることが予想される。

【００４８】そこで、位置合わせ処理部１５１では、抽出特徴データを登録特徴データを得たときと同じ位置状態で得たデータとなるように、位置合わせ処理を行う。この処理によって、照合をより確実に行うことができる。位置合わせ処理の具体的な手法は後述する。

【００４９】相違度計算部１５２は、位置合わせ処理部１５１の出力信号から抽出特徴データと登録特徴データとの相違度を計算する。当然のことながら、この相違度が小さいほど特徴測定ユニット１４及びデータ縮退ユニット１３において、特徴が抽出された被認証者は、予めファイルシステム１６の登録されている使用者本人である可能性が高いことになる。

【００５０】比較部１５３は、相違度計算部１５２で求められた相違度をあるしきい値ＴＨと比較することによって、被認証者が登録されている本人かどうか、つまりアクセス権を有する使用者か否かを判定する。

【００５１】上述したこの第１の実施の形態の構成において、コンピュータシステム１１を介してコンピュータネットワークシステム１０にアクセスしようとする使用者は、まず、そのコンピュータシステム１１に接続された特徴計測ユニットを介して指の特徴を入力する。特徴計測ユニット１４及びデータ縮退ユニット１３により得られた抽出特徴データは、通信網１２を介して前記図５に示されるような構成を有する照合サーバ１５に転送され、この照合サーバ１５において予めファイルシステム１６に登録されている登録特徴データと比較照合される。この比較照合によって、使用者のアクセス権の有無が判定される。

【００５２】照合サーバ１５での照合処理は、図６に示すフローチャートに従って行われる。先ず、位置合わせ処理部１５１で位置合わせ処理が行われる。即ち、アクセスを要求するコンピュータシステム１１から送られた

抽出特徴データである信号パターンＡ（ｉ）が入力される（ステップＳ１１）。更に、この信号パターンＡ（ｉ）と、照合サーバ１５がファイルシステム１６から読み出した登録特徴データである登録信号パターンＡｄ（ｉ）とを用い、Ａ（ｉ）をｍだけずらした信号パターンＡ（ｉ＋ｍ）と登録信号パターンＡｄ（ｉ）との２乗誤差を所定の範囲にわたって加算される（ステップＳ１２）。

【００５３】この加算値をＳ（ｍ）とすると、これはｍの値の範囲によって次式（１）（２）のいずれかとなる。なお、ｍ≧０は指を例えば指先方向にシフトした状態に相当するものする、ｍ＜０は指をこれと逆方向つまり根元方向にシフトた状態に相当する。

【００５４】

【数１】

m≧0のとき

$$S(m)=\frac{1}{N-m}\sum_{i=1}^{N-m}\{A(i+m)-Ad(i)\}^2 \qquad (1)$$

m＜0のとき

$$S(m)=\frac{1}{N+m}\sum_{i=-m+1}^{N}\{A(i+m)-Ad(i)\}^2 \qquad (2)$$

【００５５】この加算値Ｓ（ｍ）は、Ａ（ｉ＋ｍ）とＡｄ（ｉ）との一致度を表わすパラメータであり、このＳ（ｍ）の値が小さいほど一致していることを示す。ｍを所定の範囲で変化させ、Ｓ（ｍ）の値が最小となるときのｍを位置ずれ量Ｍとし、この位置ずれ量ＭだけシフトしたパターンＡ（ｉ）を、即ち、パターンＡ（ｉ＋Ｍ）において位置合わせができると判定する（ステップＳ１３）。次に、相違度計算部１５２において、相違度Ｅが次式（３）（４）により求められる（ステップＳ１４）。

【００５６】

【数２】

M≧0のとき

$$E=\sum_{i=1}^{N-M}\{A(i+M)-Ad(i)\}^2 \Big/ \sum_{i=1}^{N-M}Ad(i)^2 \qquad (3)$$

M＜0のとき

$$E=\sum_{i=-M+1}^{N}\{A(i+M)-Ad(i)\}^2 \Big/ \sum_{i=-M+1}^{N}Ad(i)^2 \qquad (4)$$

【００５７】このような式で求められる相違度Ｅは、位置合わせされた入力信号パターンＡ（ｉ＋Ｍ）と登録信号パターンＡｄ（ｉ）の２乗誤差を所定の範囲にわたって加算したものを同じ範囲の登録信号パターンＡｄ（ｉ）の２乗和で正規化したもを示す。この相違度Ｅは位置合わせされた入力信号パターンＡ（ｉ＋Ｍ）と登録信号パターンＡｄ（ｉ）との相違度を表したもので、Ｅの値が大きいほど両信号の違いが大きく、値が小さいほど両信号が似ていることを示す。

【００５８】次に、比較部１５３において、相違度Ｅが予め定められたしきい値ＴＨと比較され（ステップＳ１５；Ｓ１６）、Ｅ≦ＴＨならば両信号は一致しており、

アクセスを使用として使用者である被認証者を本人と判断して照合処理を終了する（ステップＳ１７）。また、Ｅ＞ＴＨならば両信号が一致していないと判断し、被認証者を他人と判断して照合処理を終了する（ステップＳ１８）。

【００５９】前記ステップＳ１７で被認証者を本人と判断すると、照合サーバ１５はその被認証者つまり使用者にアクセス許可を与える。照合サーバ１５は、全てのネットワーク上のアクセス条件が設定されており、ネットワーク内のあるコンピュータシステムが同じネットワーク内の他のコンピュータシステム（サービス）にアクセスを要求する際にも、上述のようにして抽出された特徴データを使用者識別子を用い、照合・判定処理を行うことができる。

【００６０】以上説明したように、この第１の実施の形態によれば人間の身体的特徴を示す（この第１の実施の形態では指の指紋）特徴を抽出して得られる特徴データを使用者識別子として、予め登録されている特徴データと比較照合することでネットワークシステムに対するアクセス権の有無が判定される。

【００６１】これにより、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護を実現できる。また、特徴データの抽出には使用者が例えば実施の形態で説明したような線状電極アレイ上に指を押し付けるという簡単な操作を行えばよく、パスワード入力のような煩雑な入力操作を必要としないので、アクセス操作における使用者の負担を大きく軽減することができる。

【００６２】又、この第１の実施の形態で用いられる特徴データは縮退されたデータであり、一般的な指紋画像を用いるものに比べて、データ量が約１０分の１となり、図１のコンピュータネットワーク上での通信網１２を介しての転送や、照合サーバ１５での照合等の処理を高速で行うことができる。同様に、照合処理に必要とされるファイルシステム１６の容量も従来の約１０分の１でよい。

【００６３】前記特徴データの抽出には、従来適用されている光学方法では、図７（ａ）に示されるような各種処理が必要とされる。先ず、光学センサによって２次元情報である指画像が取り込まれ、取り込まれた指画像の指の横方向の画素情報が加算される（ステップＳ２１，Ｓ２２）。この後、バンドパスフィルタを用いて加算された情報の高周波成分及び低周波成分が除去され、特徴データとして出力される（ステップＳ２３，Ｓ２４）。

【００６４】一方、前述した電極アレイを用いた方法では、図７（ｂ）に示されるように、指の抵抗値分布の検出（ステップＳ３１）と、高周波成分・低周波成分の除去（ステップＳ３２）とを行った後に特徴データが出力され（ステップＳ３３）、従来の光学方法に比べて少ない処理で特徴データを出力することができる。このため、各コンピュータシステム１１に接続されたデータ縮退ユニット１３及び特徴計測ユニット１４において迅速な特徴データの抽出が可能となる。

【００６５】この第１の実施の形態においては、人間の身体的特徴を示す縮退された特徴データとして指の指紋の一次元射影を用いたが、この他、指の輪郭や、フーリエ変換を用いて求めた指紋情報を適用することもできる。

【００６６】また、一度このようにしてネットワークへのアクセスが認められた場合、指の特徴データをあるコンピュータシステムから他のコンピュータシステムにアクセスする際の使用者識別子として使用することにより、他のコンピュータシステムにアクセスする際に従来必要としていた複数種類のパスワード入力のような煩わしい手順を簡略化することができる。

【００６７】前述した電極アレイ式では、特徴計測ユニットと縮退ユニットとが一体のユニットとなる構成であった。しかし、例えば、１次元射影を検出する光学式の装置を適用しても良い。この場合には、図８（ａ）に示されるように、特徴計測ユニットとデータ縮退ユニットとを異なるユニットで構成することができる。同図に示されるように、特徴計測ユニットは、光学式指紋測定器により構成され、データ縮退ユニットは、一次元射影計算部及びフィルタリング・Ａ／Ｄ変換部により構成される。

【００６８】光学式指紋画像測定器は、図８（ｂ）に示されるような２次元の指紋画像の測定を行い、測定された画像情報を一次元射影計算部に送る。一次元射影計算部では、２次元の画像情報を一次元の情報に計算すると共に、フィルタリング処理や、Ａ／Ｄ変換を行うことにより、抽出された特徴を含む縮退データを出力する。

【００６９】前述した第１の実施の形態では、データ縮退ユニット１３を介してコンピュータシステム１１と特徴計測ユニット１４とが接続された構成となっているが、データ縮退ユニット１３及び特徴計測ユニット１４をコンピュータシステム１１に組み込んだ構成としてもよい。例えば、特徴計測ユニット１４と同様の機能を有する特徴計測部をコンピュータシステム１１のキーボード上に配設してもよい。

【００７０】このように、データ縮退ユニット１３と特徴計測ユニット１４とを、特徴抽出部としてコンピュータシステム１１に組み込ませた場合、前述したコンピュータネットワークシステムは図９に示されるような構成となる。

【００７１】ここでは、前述した第１の実施の形態と同様に、複数のコンピュータシステム２１（２１－１～２１－３）が通信網２２を介して相互に接続されている。各コンピュータシステム２１には、使用者の身体的特徴（特徴データ）を抽出する特徴抽出部２７（２７－１～２７－３）がそれぞれ内蔵されている。この特徴抽出部

２７の機能は、前述した特徴計測ユニット１４及びデータ縮退ユニット１３の有する機能と同様であり、抽出された特徴データは、縮退されたデータである。

【００７２】通信網２２には、更に、各特徴計測ユニット２４により測定された特徴データに基づいてコンピュータネットワークシステムに対する使用者のアクセス権の有無を識別する照合サーバ２５が接続されている。

【００７３】図９に示されるコンピュータネットワークシステム２０における動作は、前述した第１の実施の形態の動作と同様であるので詳細な説明は省略する。又、コンピュータネットワークシステム２０においても、第１の実施の形態と同様の効果を得ることができる。

【００７４】次に、この発明に係るコンピュータネットワークシステムの第２の実施の形態を説明する。この第２の実施の形態では、この発明をワークフローシスム（workflow system ）に適用する。

【００７５】図１０は、この第２の実施の形態におけるワークフローの処理を示すフローチャートである。この第２の実施の形態に係るコンピュータネットワークシステムは、前記図１に示される第１の実施の形態の構成と同様の構成を有する。

【００７６】このコンピュータネットワークシステムは、ワークシステム上に設定された一連の仕事の流れを運用するワークフローシステムであり、電子承認が必要な処理を行うコンピュータシステム１１に、身体的特徴を抽出するための、データ縮退ユニット１３及び特徴抽出ユニット１４が接続されており、照合サーバ１５のファイルシステム１６には承認権利を有する人の特徴データ（例えば、指の指紋情報）および処理条件が登録されている。

【００７７】以下、図１０を用いて具体的に処理の流れを説明する。尚、ここでは、前述した第１の実施の形態と同様に特徴データとして、人間の指の指紋情報を適用する。

【００７８】設定された一連の仕事の流れの中で、承認手続き要求が発生した場合、要求された使用者のコンピュータシステム１１は通信網１２を介して承認手続き要求を受信する（ステップＳ４１）。承認者は、受信した要求手続きを端末に表示させ、特徴計測ユニット１４を介して指の特徴を入力する（ステップＳ４２）。抽出された特徴データは通信網１２を介して照合サーバ１５へ送信される。

【００７９】照合サーバ１５では、図６を用いて説明した照合処理が行われる。これにより、ファイルシステム１５に予め承認権利有資格者として登録してある特徴データと、送信された抽出特徴データが一致した場合、承認・非承認手続きを実行することが可能であるとして前記コンピュータシステム１１に許可が与えられる（ステップＳ４３）。承認手続き処理が実行された後、通信網１２を介して次の処理に該当するコンピュータシステム１１に処理データが送られる（ステップＳ４４，Ｓ４５）。

【００８０】尚、ここでは承認手続きに関して説明したが、計算や文書追加等他の処理に関しても、処理実行者を限定したい場合は同様にこの発明を適用することが可能である。

【００８１】さらに、コンピュータネットワークシステム上に設定された一連の仕事の流れを運用するワークフローシステムにこの発明を適用すれば、予め設定した条件によって承認・非承認の判定を行う判定処理の際に、予め登録してある指の特徴データと判定時に入力された指の特徴データが一致した場合のみに判定処理を行うことができるため、簡単な操作で確実な電子承認が可能となる。

【００８２】そして、この発明における指の特徴抽出手段では、線状電極アレイのアレイ方向に沿って使用者の指が接触することによる隣接電極間の抵抗値の分布から指の特徴を抽出して、指の長手方向に沿った一次元の特徴抽出データを出力するものであることから、指紋を２次元の画像として検出する指紋センサに比較して特徴データのデータ量が著しく少ないため、コンピュータネットワークシステム上での転送や登録されている特徴データとの照合処理を高速に行うことができ、従って迅速に個人認証を行うことが可能となる。

【００８３】次に、この発明に係るコンピュータネットワークシステムの第３の実施の形態を図１１～図１３を参照して説明する。図１０に示されるコンピュータネットワークシステム３０は、複数のコンピュータシステム３１（３１－１～３１－３）が通信網３２を介して相互に接続されている。各コンピュータシステム３１にはそれぞれデータ縮退ユニット３３（３３－１～３３－３）を介し、使用者の身体的特徴（特徴データ）を計測する特徴計測ユニット３４（３４－１～３４－３）がそれぞれ接続されている。このデータ縮退ユニット３３及び特徴計測ユニット３４により使用者の身体的特徴が電気信号として抽出される。

【００８４】尚、この実施の形態では、抽出される身体的特徴を特に限定しないが、例えば、前述した第１の実施の形態と同様に、使用者の指の指紋情報（一次元射影）を測定してもよく、この他、フーリエ変換、輪郭抽出による縮退された特徴データを適用することができる。更に、前記第１の実施の形態と同様に、接続されるコンピュータシステムの数はこれに限定されない。

【００８５】前記図１に示されるコンピュータネットワークシステム１０と異なる第１の点は、身体的特徴を照合するための照合サーバ１５、及びこの照合サーバにより参照される登録特徴データを格納するファイルシステム１６がもうけられていないことである。第２の相違点は、通信網３２に接続されている各コンピュータシステム３１に、それぞれファイルシステム３５（３５－１～

３５－３）が接続されていることである。

【００８６】このファイルシステム３５は、アクセス権の有無を判定するための照合処理の際に参照される登録特徴データ、及び処理対象となる各種ファイル・データを格納する。従って、この第３の実施の形態では、特徴データの抽出に応じ、先ず、各コンピュータシステム３１においてアクセス権の有無を判定するための照合処理を行うことができる。

【００８７】次に、図１２及び図１３に示されるフローチャートを参照して、この第３の実施の形態のコンピュータネットワークシステム３０のファイルアクセス動作について説明する。

【００８８】コンピュータネットワークシステム３０において、任意のコンピュータシステム３１でファイルのアクセス要求が発生すると、このコンピュータ３１では、特徴計測ユニット３４を用いて身体的特徴、例えば指の指紋等を入力するように要求される。ここで、使用者の指等が特徴ユニット３４に載置されると、前述した第１の実施の形態における処理と同様に特徴計測ユニット３４及びデータ縮退ユニット３３により縮退された特徴データが抽出される（ステップＳ５１，Ｓ５２）。

【００８９】抽出された特徴データ（抽出特徴データ）は、アクセス要求の発生した日時や、パスワード等の使用者識別子に付加される（ステップＳ５３）。尚、日時やパスワード等の識別子を付与せず、縮退された抽出特徴データのみを用いても良い。

【００９０】次に、コンピュータシステム３１では、アクセス要求されたファイルがこのコンピュータシステム３１に接続されているファイルシステム３５に格納されているか否か判定する（ステップＳ５４）。ここで、ファイルシステム３５にアクセス要求されたファイルが格納されている場合、ファイルシステム３５に格納されている登録特徴データと、前記抽出特徴データ及び使用者識別子とが同一であるか照合処理が行われる（ステップＳ５６）。

【００９１】ここで行われる照合処理は、前述した第１の実施の形態における照合処理等を適用することができる。照合処理の結果が一致である場合、使用者に対し、ファイルアクセスが許可される（ステップＳ５７）。一致でない場合、ファイルアクセスが不可能である通知等がなされた後、ファイルアクセス要求に応じた処理が終了する。

【００９２】前記ステップＳ５４において、ファイルシステム３５にアクセス要求されたファイルが格納されていない場合、コンピュータシステム３１は、アクセス要求するファイルのファイル名等と共に前記抽出特徴データ及び使用者識別子を、通信網３２を介して他のコンピュータシステムに送出する（ステップＳ５８）。この後、抽出特徴データ等を送出した送り先のコンピュータシステムからの応答を受信し、アクセスの可否に応じて前述したような処理を行う（ステップＳ５９）。

【００９３】尚、後述するがアクセス可の場合、アクセス要求したファイルが送られるので、これをファイルシステム３５に格納する等の処理も行われる。次に、前記ステップＳ５８において送出された各種データを受信したコンピュータシステム３１の処理を図１３を参照して説明する。

【００９４】コンピュータシステム３１は、他のコンピュータシステムから、アクセス要求するファイルのファイル名等と共に前記抽出特徴データ及び使用者識別子を受信すると、アクセス要求されているファイルが自コンピュータシステム３１に接続されているファイルシステム３５に格納されているか否か判定する（ステップＳ６１，Ｓ６２）。ここで、ファイルシステム３５に要求されたファイルが格納されていない場合、この旨を要求元のコンピュータシステムに通知する（ステップＳ６３）。

【００９５】前記ステップＳ６２において、アクセス要求されたファイルがファイルシステム３５に格納されている場合、ステップＳ６１において受信した抽出特徴データ及び使用者識別子を用い、要求元の使用者にファイルアクセス権が有るか否かを決定するための照合処理を行う（ステップＳ６４，Ｓ６５）。照合結果が一致である場合、要求元のコンピュータシステムに対し、アクセス権を有することを通知すると共に、アクセス要求されたファイルを送出する（ステップＳ６６）。照合結果が不一致である場合、ファイルのアクセス権が無いことを要求元のコンピュータシステムに通知する（ステップＳ６７）。

【００９６】以上説明したように、この第３の実施の形態によれば人間の身体的特徴を示す特徴を抽出して得られる特徴データを使用者識別子として、予め登録されている特徴データと比較照合することでネットワークシステムに対するアクセス権の有無が判定される。これにより、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護を実現できる。

【００９７】特に、この第３の実施の形態では、通信網３２に接続されている各コンピュータシステムにおいて、先ず、ファイルアクセス要求に応じたアクセス権の有無判定処理が単独で行われ、アクセス要求されたファイルがファイルシステムに格納されていない時のみ、通信網３２を介して他のコンピュータシステムにおいてアクセス権の有無判定処理が行われる。このため、アクセス権の有無判定処理を行う度に通信網３２を介してデータの送受を行う必要はなく、通信網３２上のデータの通信効率を向上することが可能となる。

【００９８】又、この第３の実施の形態で用いられる特徴データは、前記第１の実施の形態と同様に縮退されたデータであり、一般的な指紋画像を用いるものに比べ

て、データ量を節約することができる。従って、データの転送や処理を高速に行うことができる。

【００９９】次に、この発明に係るコンピュータネットワークシステムの第４の実施の形態を図１４及び図１５を参照して説明する。図１４に示されるコンピュータネットワークシステム４０は、基本的に前記図１に示されるコンピュータネットワークシステム１０と同様であるので詳細な説明は省略する。但し、このコンピュータネットワークシステム４０は、前述した第３の実施の形態と同様に、通信網４２に接続されている各コンピュータシステム４１に、それぞれファイルシステム４７（４７－１～４７－３）が接続されている。

【０１００】但し、このファイルシステム４７は、処理対象となる各種ファイル・データのみを格納する。従って、この第４の実施の形態では、前記第１の実施の形態と同様に、特徴データの抽出に応じ照合サーバ４５に抽出特徴データが送られる。そして、この照合サーバ４５において、アクセス権の有無を判定するための照合処理が行われる。

【０１０１】このコンピュータネットワークシステム４０における、ファイルアクセスに応じた、コンピュータシステム４１及び照合サーバ４５の処理を図１５のフローチャートに示す。

【０１０２】コンピュータネットワークシステム４０において、任意のコンピュータシステム４１でファイルのアクセス要求が発生すると、このコンピュータ４１では、特徴計測ユニット４４を用いて身体的特徴、例えば指の指紋等を入力するように要求される。ここで、使用者の指等が特徴ユニット４４に載置されると、前述した第１の実施の形態における処理と同様に特徴計測ユニット４４及びデータ縮退ユニット４３により縮退された特徴データが抽出される（ステップＳ７１，Ｓ７２）。

【０１０３】抽出された特徴データ（抽出特徴データ）は、アクセス要求の発生した日時や、パスワード等の使用者識別子に付加され、通信網４２を介して照合サーバ４５に送出される（ステップＳ７３，Ｓ７４）。尚、日時やパスワード等の識別子を付与せず、縮退された抽出特徴データのみを用いても良い。

【０１０４】次に、照合サーバ４５では、抽出特徴データ及び使用者識別子の受信に応じ、ファイルシステム４５に格納されている登録特徴データと、前記抽出特徴データ及び使用者識別子とが同一であるか照合処理が行われる（ステップＳ７５，Ｓ７６）。ここで行われる照合処理は、前述した第１の実施の形態における照合処理等を適用することができる。照合処理の結果が一致である場合、使用者に対し、ファイルアクセスが許可され、この旨が通知される（ステップＳ７７，Ｓ７８）。一致でない場合、ファイルアクセス権無しと判断されこの旨が通知される（ステップＳ７９，７８）。

【０１０５】以上説明した、この第４の実施の形態によれば前記第１の実施の形態と同様の効果を得ることができる。即ち、人間の身体的特徴を示す特徴を抽出して得られる特徴データを使用者識別子として、アクセス権の有無が判定されので、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護を実現できる。又、用いられる特徴データは、前記第１の実施の形態と同様に縮退されたデータであり、一般的な指紋画像を用いるものに比べて、データ量を節約することができる。従って、データの転送や処理を高速に行うことができる。

【０１０６】

【発明の効果】以上詳述したように、この発明によれば、コンピュータシステムにおいて、身体的特徴データを用いることにより、使用者からのアクセス要求に応じてアクセス権の有無を判別する処理を高速に行うことができ、且つ、確実に機密保護を維持することが可能となる。

【０１０７】又、この発明によれば、コンピュータネットワークシステムにおいて使用される個人認証装置において、容易な操作で確実な認証処理を行い、使用者の負担を軽減することができる。

【０１０８】特に、人間の身体的特徴を示す特徴を抽出して得られる特徴データを使用者識別子として、予め登録されている特徴データと比較照合することでネットワークシステムに対するアクセス権の有無が判定される。これにより、特徴データが登録されていない他人によるアクセスに対して、パスワードを用いるよりも確実な機密保護を実現できる。また、特徴データの抽出には使用者が例えば実施の形態で説明したような線状電極アレイ上に指を押し付けるという簡単な操作を行えばよく、パスワード入力のような煩雑な入力操作を必要としないので、アクセス操作における使用者の負担を大きく軽減することができる。

【０１０９】又、この特徴データは縮退されたデータであり、一般的な指紋画像を用いるものに比べて、データ量が約１０分の１となり、コンピュータネットワーク上での通信網を介しての転送や、照合サーバ等での照合等の処理を高速で行うことができる。同様に、照合処理に必要とされるファイルシステムの容量も従来の約１０分の１でよい。

【図面の簡単な説明】

【図１】この発明の第１の実施の形態に係るコンピュータネットワークシステムの概略構成を示すブロック図。

【図２】前記第１の実施の形態における特徴計測及びデータ縮退ユニットの概略構成を示す図。

【図３】前記第１の実施の形態における特徴計測及びデータ縮退ユニットの等価回路の一例を示す図。

【図４】前記第１の実施の形態における特徴計測及びデータ縮退ユニットにより検出される、縮退済みの指の特徴パターンである、隣接電極間の抵抗値の分布例を示す

図。

【図５】前記第１の実施の形態における照合サーバの構成を示すブロック図。

【図６】前記照合サーバの動作を説明するためのフローチャート。

【図７】特徴データを抽出するための従来の光学方法における処理と、前記第１の実施の形態における電極アレイ方法の処理を比較するフローチャート。

【図８】光学式の一次元射影検出装置を前記第１の実施の形態に適用する場合を説明するための図。

【図９】前記第１の実施の形態に係るコンピュータネットワークシステムの変形例を示す図。

【図１０】この発明の第２の実施の形態に係るワークフロー処理を説明するためのフローチャート。

【図１１】この発明の第３の実施の形態に係るコンピュータネットワークシステムの概略構成を示すブロック図。

【図１２】前記第３の実施の形態のコンピュータネットワークシステムにおいて、ファイルアクセス要求の生じたコンピュータシステムの処理を示すフローチャート。

【図１３】前記第３の実施の形態のコンピュータネットワークシステムにおいて、他のコンピュータシステムからファイルアクセス要求を受けたコンピュータシステムの処理を示すフローチャート。

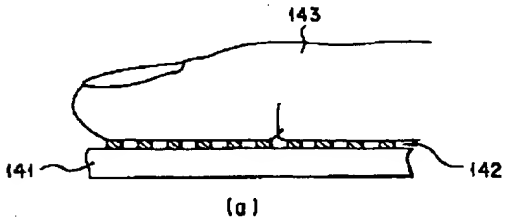
【図１４】この発明の第４の実施の形態に係るコンピュータネットワークシステムの概略構成を示すブロック図。

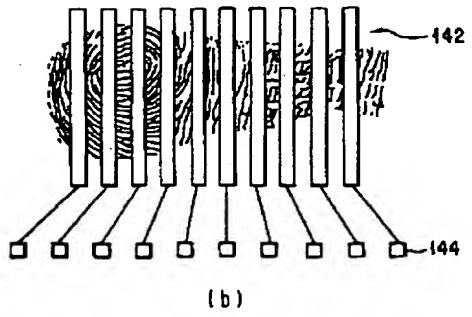
【図１５】前記第４の実施の形態のコンピュータネットワークシステムにおけるコンピュータシステム及び照合サーバの処理を示すフローチャート。

【符号の説明】

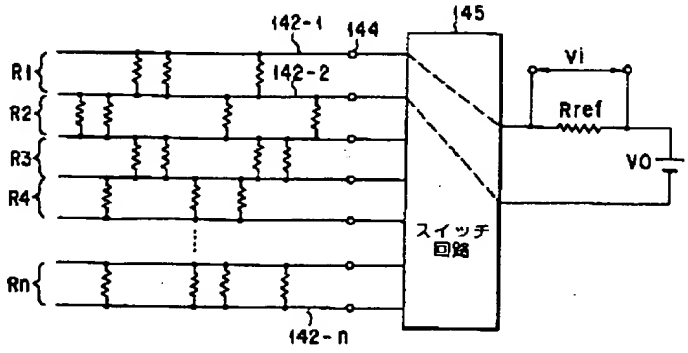
１０，２０，３０，４０…コンピュータネットワークシステム、１１（１１－１～１１－３），２１（２１－１～２１－３），３１（３１－１内３１－３），４１（４１－１～４１－３）…コンピュータシステム、１２，２２，３２，４２…通信網、１３（１３－１～１３－３），３３（３３－１～３３－３），４３（４３－１～４３－３）…データ縮退ユニット、１４（１４－１～１４－３），３４（３４－１～３４－３），４４（４４－１～４４－３）…特徴計測ユニット、１５，２５，４５…照合サーバ、１６，２６，３５（３５－１～３５－３），４６，４７（４７－１～４７－３）…ファイルシステム、２７（２７－１～２７－３）…指の特徴抽出部、５１…光学式指紋画像測定器、５２…一次元射影計算部、５３…フィルタリング・Ａ／Ｄ変換、１４１…基板、１４２…線状電極アレイ、１４３…指、１４４…端子、１４５…スイッチ回路、１５１…位置合せ処理部　１５２…相違度計算部、１５３…比較部。

【図２】

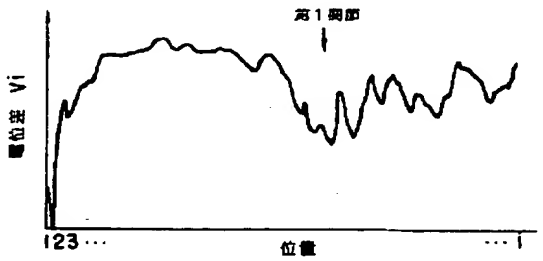




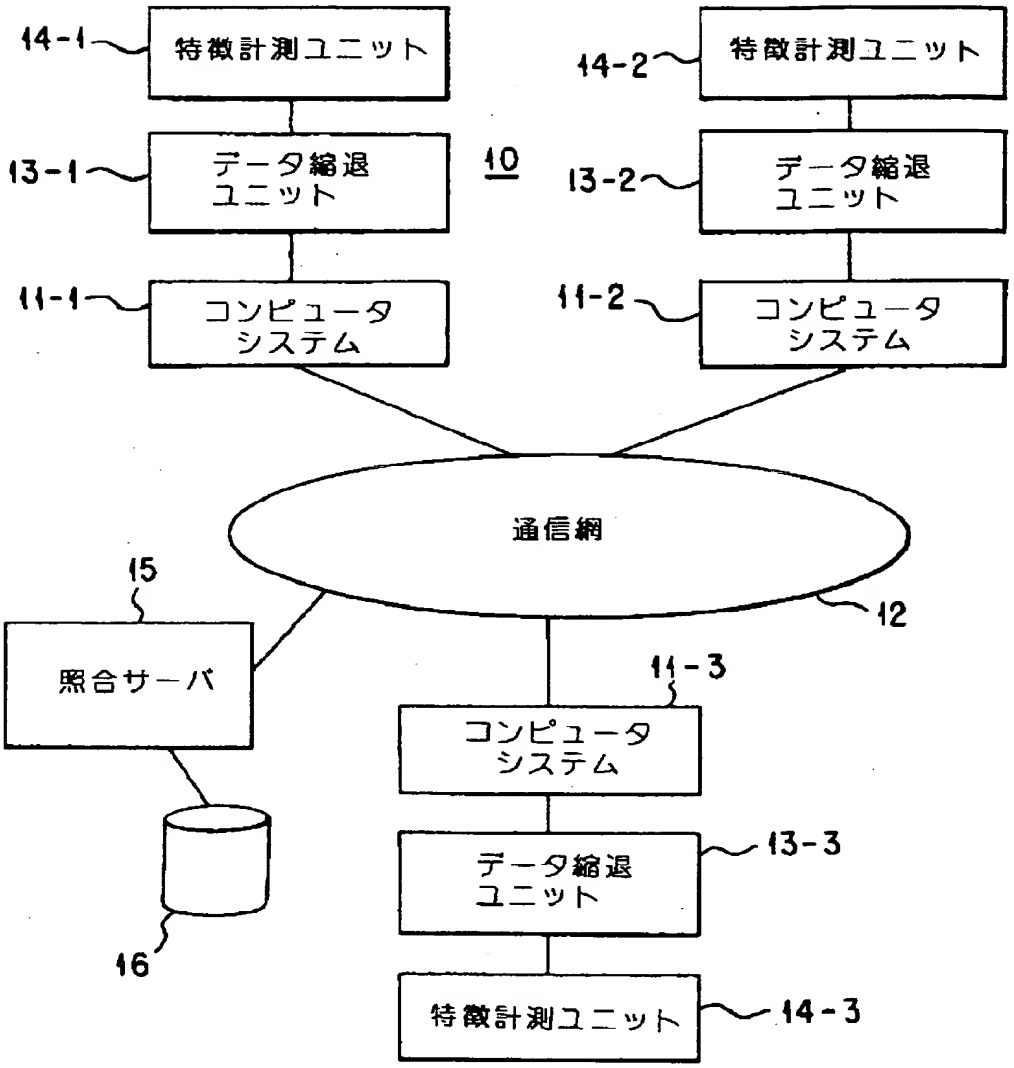
【図３】



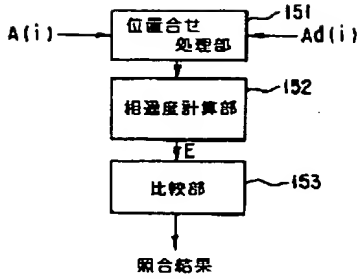
【図４】



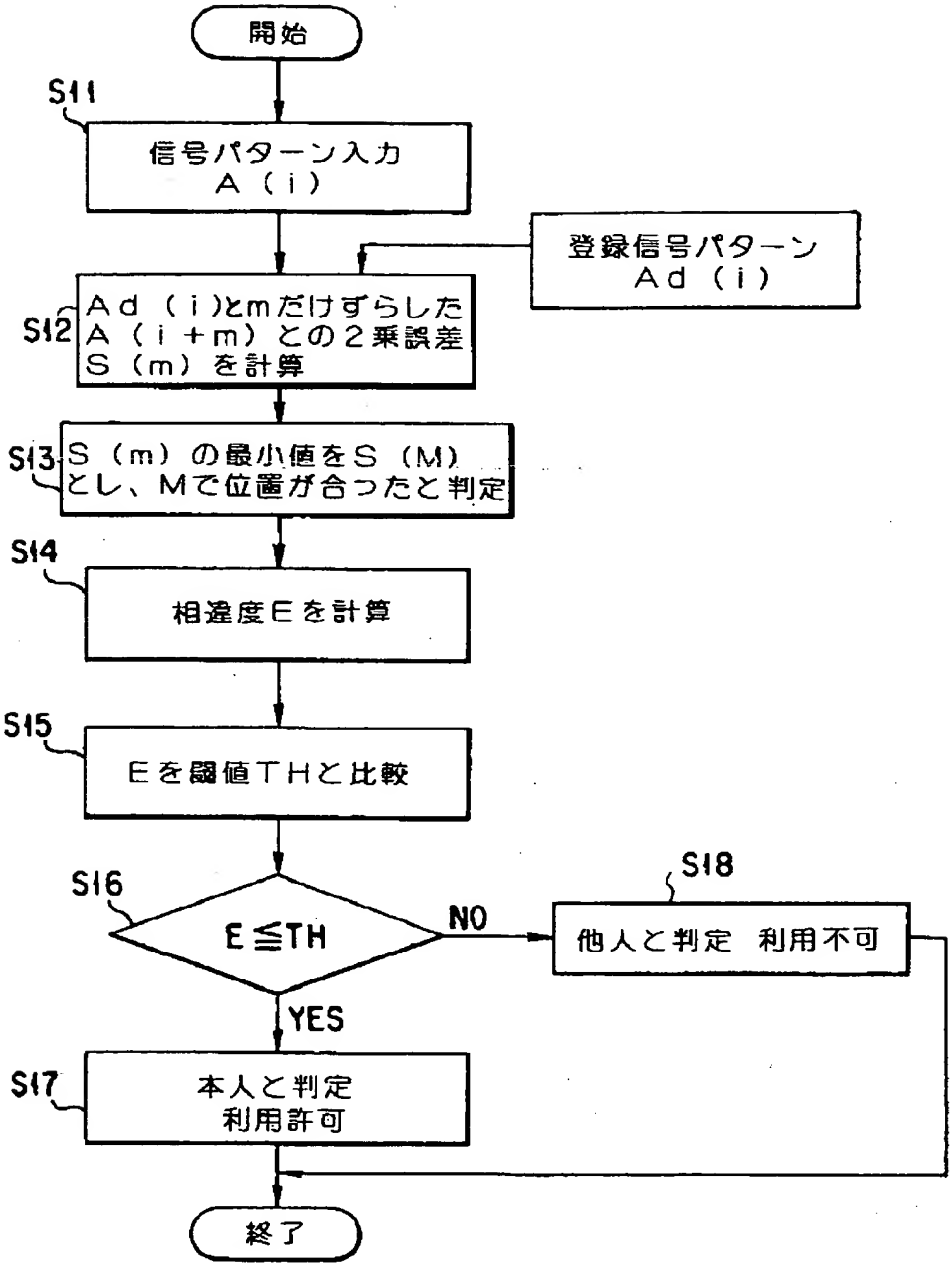
【図１】


14-1
特徴計測ユニット
14-2
特徴計測ユニット
13-1
データ縮退ユニット
10
13-2
データ縮退ユニット
11-1
コンピュータシステム
11-2
コンピュータシステム
通信網
12
15
照合サーバ
11-3
コンピュータシステム
16
データ縮退ユニット
13-3
特徴計測ユニット
14-3

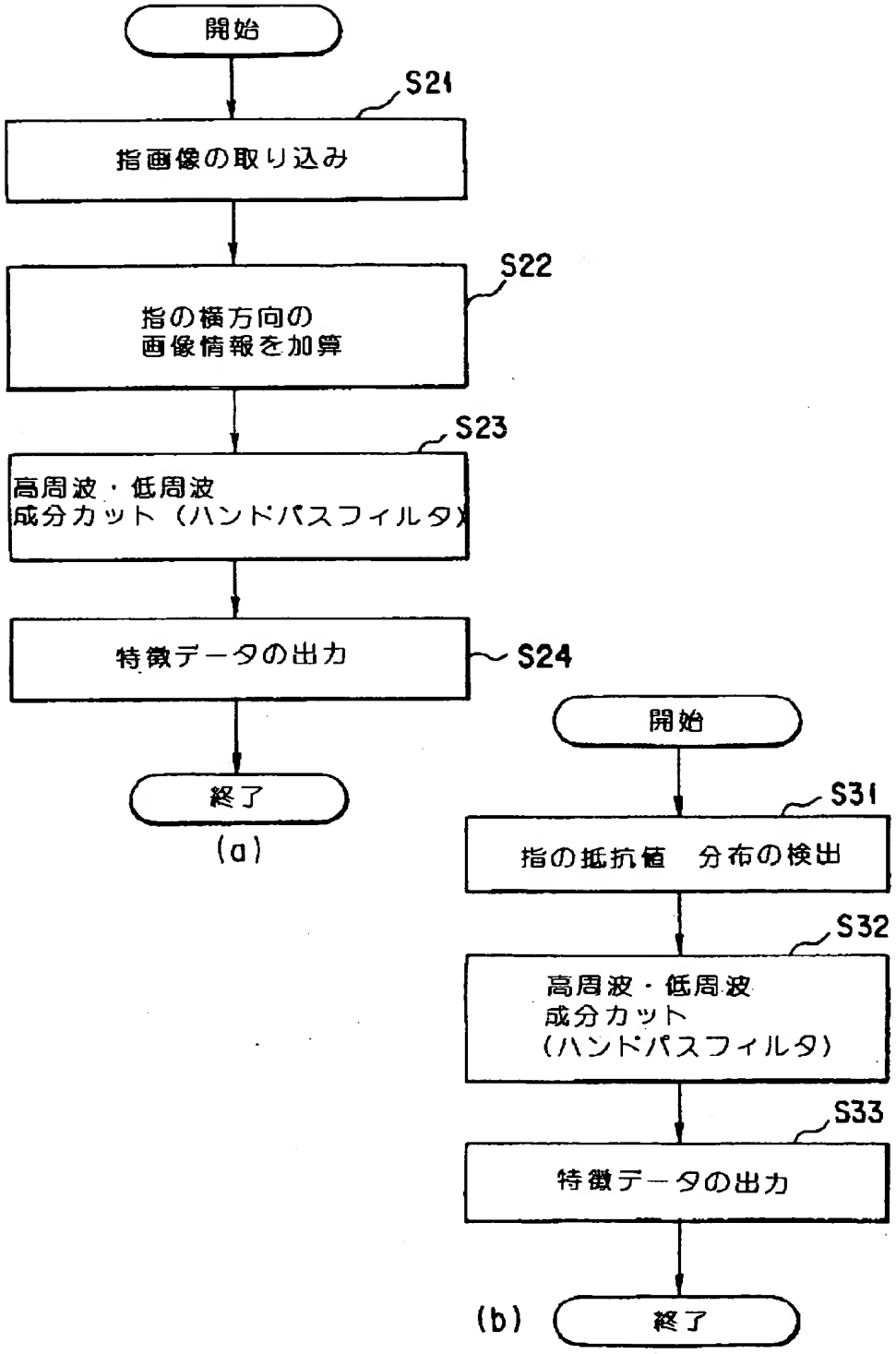
【図５】


A(i)
位置合せ処理部
151
Ad(i)
相違度計算部
152
E
比較部
153
照合結果

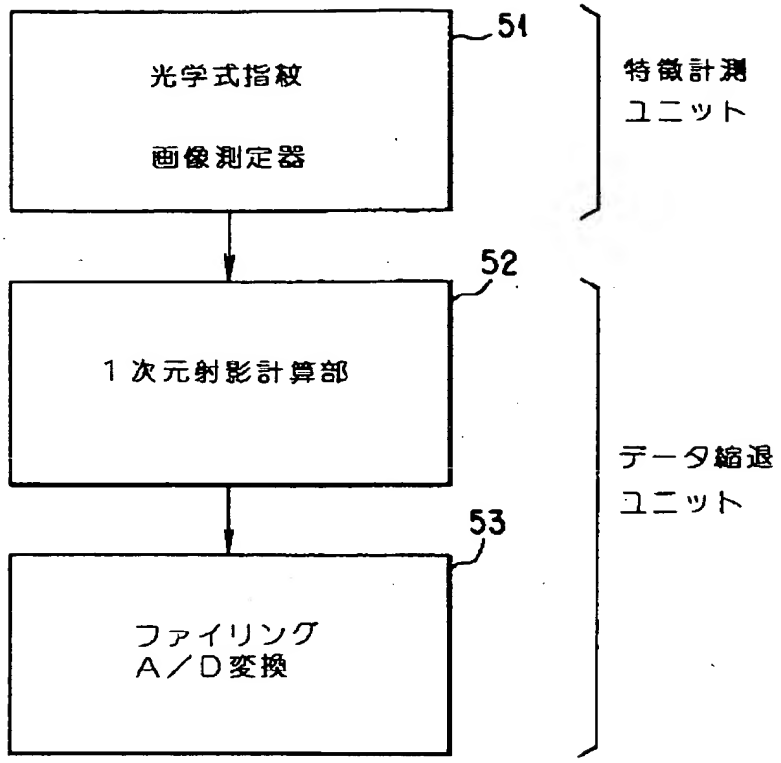
【図６】


開始
S11
信号パターン入力
A（i）
登録信号パターン
Ad（i）
S12
Ad（i）とmだけずらした
A（i＋m）との２乗誤差
S（m）を計算
S13
S（m）の最小値をS（M）
とし、Mで位置が合ったと判定
S14
相違度Eを計算
S15
Eを閾値THと比較
S16
E≦TH
NO
S18
他人と判定　利用不可
YES
S17
本人と判定
利用許可
終了

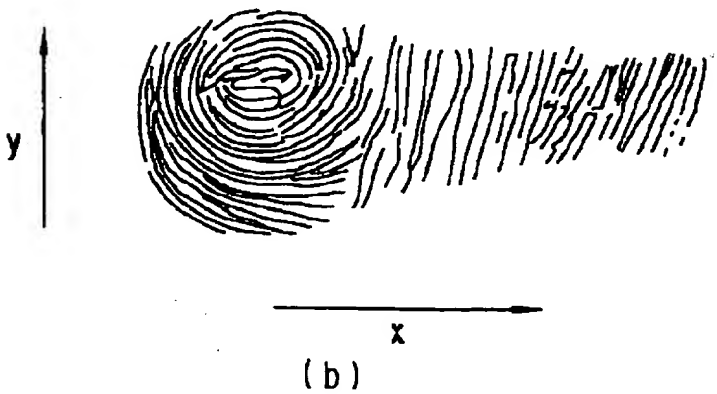
【図７】


開始
S21
指画像の取り込み
S22
指の横方向の
画像情報を加算
S23
高周波・低周波
成分カット（ハンドパスフィルタ）
特徴データの出力
S24
終了
(a)
開始
S31
指の抵抗値　分布の検出
S32
高周波・低周波
成分カット
（ハンドパスフィルタ）
S33
特徴データの出力
(b)
終了

【図８】

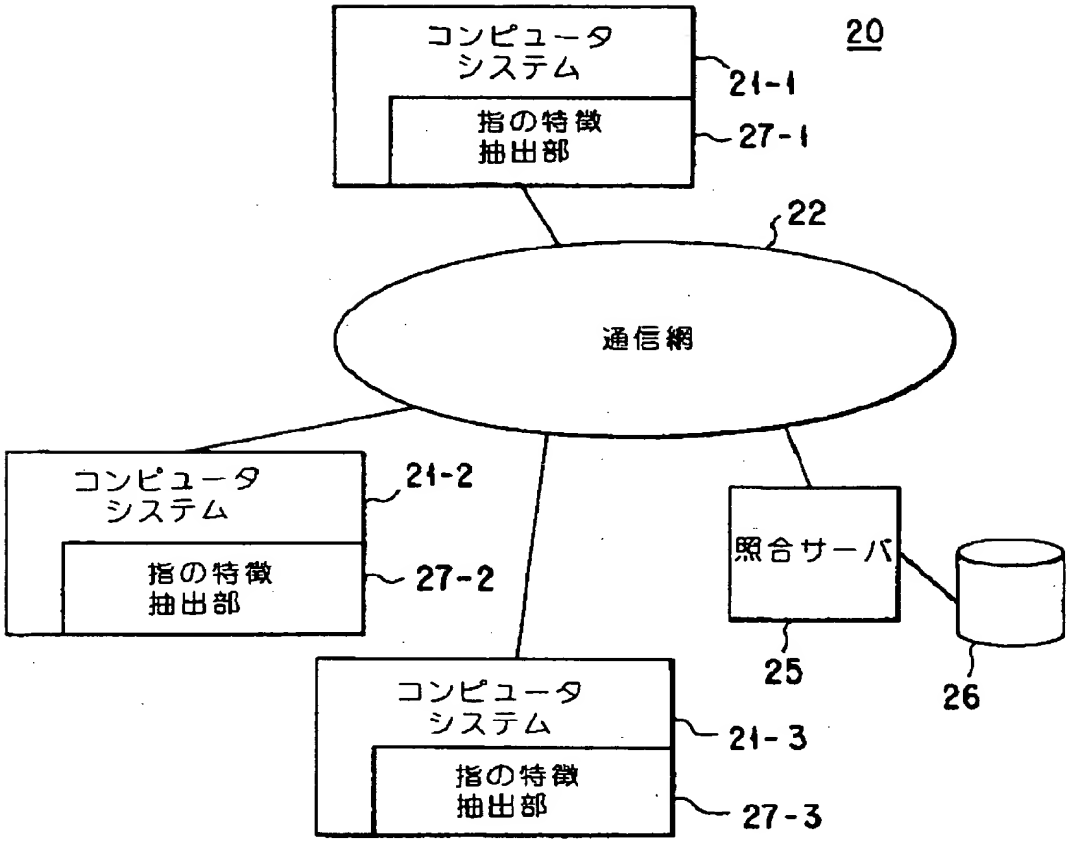

光学式指紋
画像測定器
51
特徴計測
ユニット
1次元射影計算部
52
データ縮退
ユニット
ファイリング
A／D変換
53

(a)

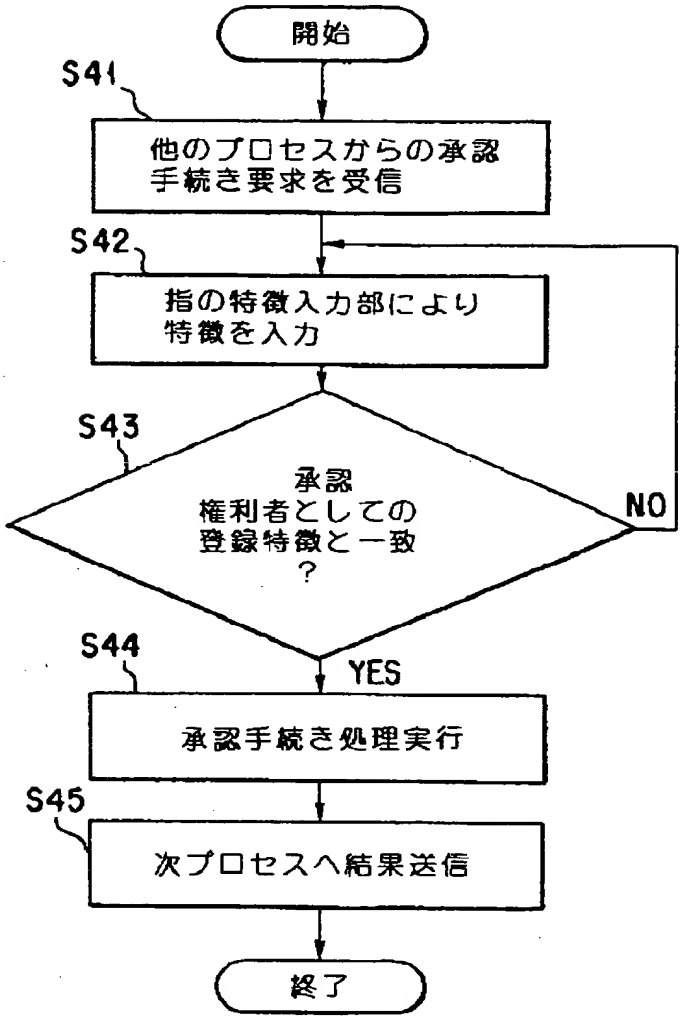

y
x

(b)

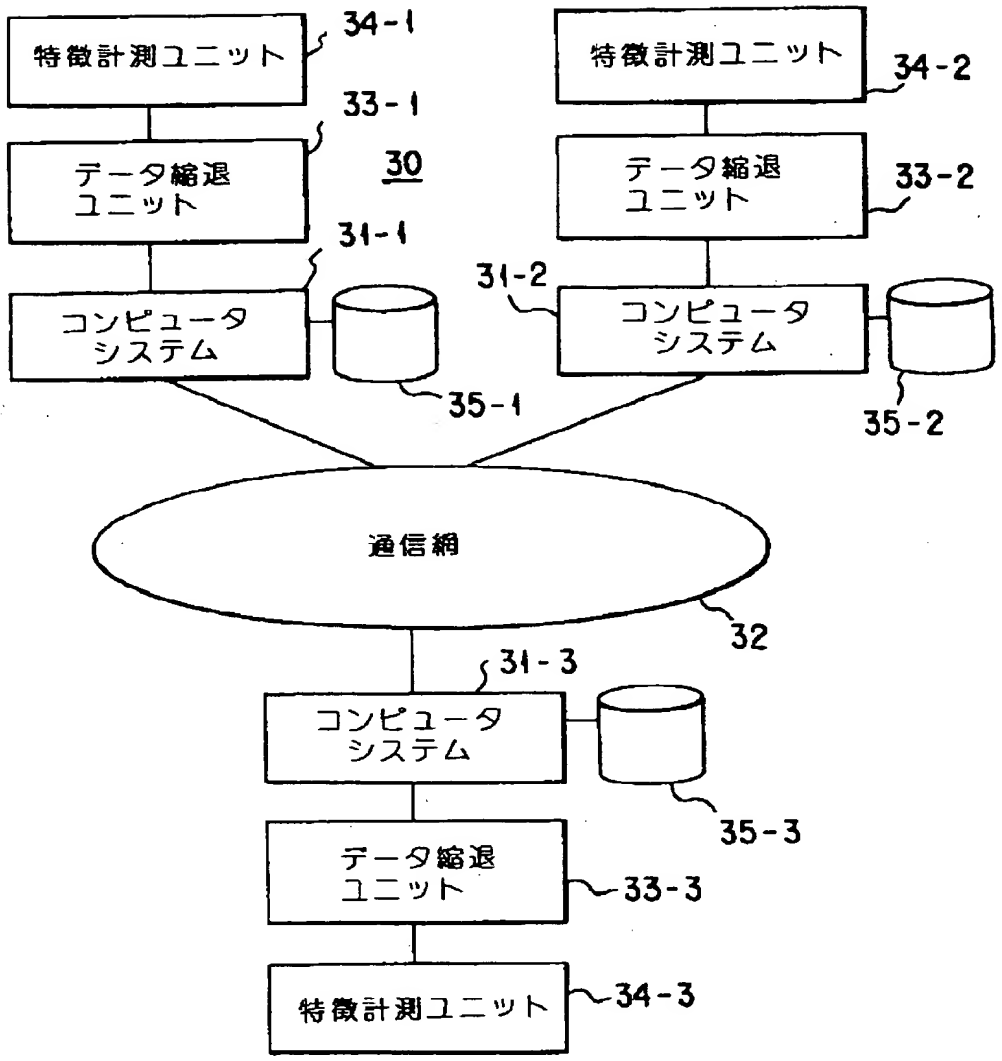
【図9】


コンピュータ
システム
21-1
指の特徴
抽出部
27-1
20
22
通信網
コンピュータ
システム
21-2
指の特徴
抽出部
27-2
照合サーバ
25
26
コンピュータ
システム
21-3
指の特徴
抽出部
27-3

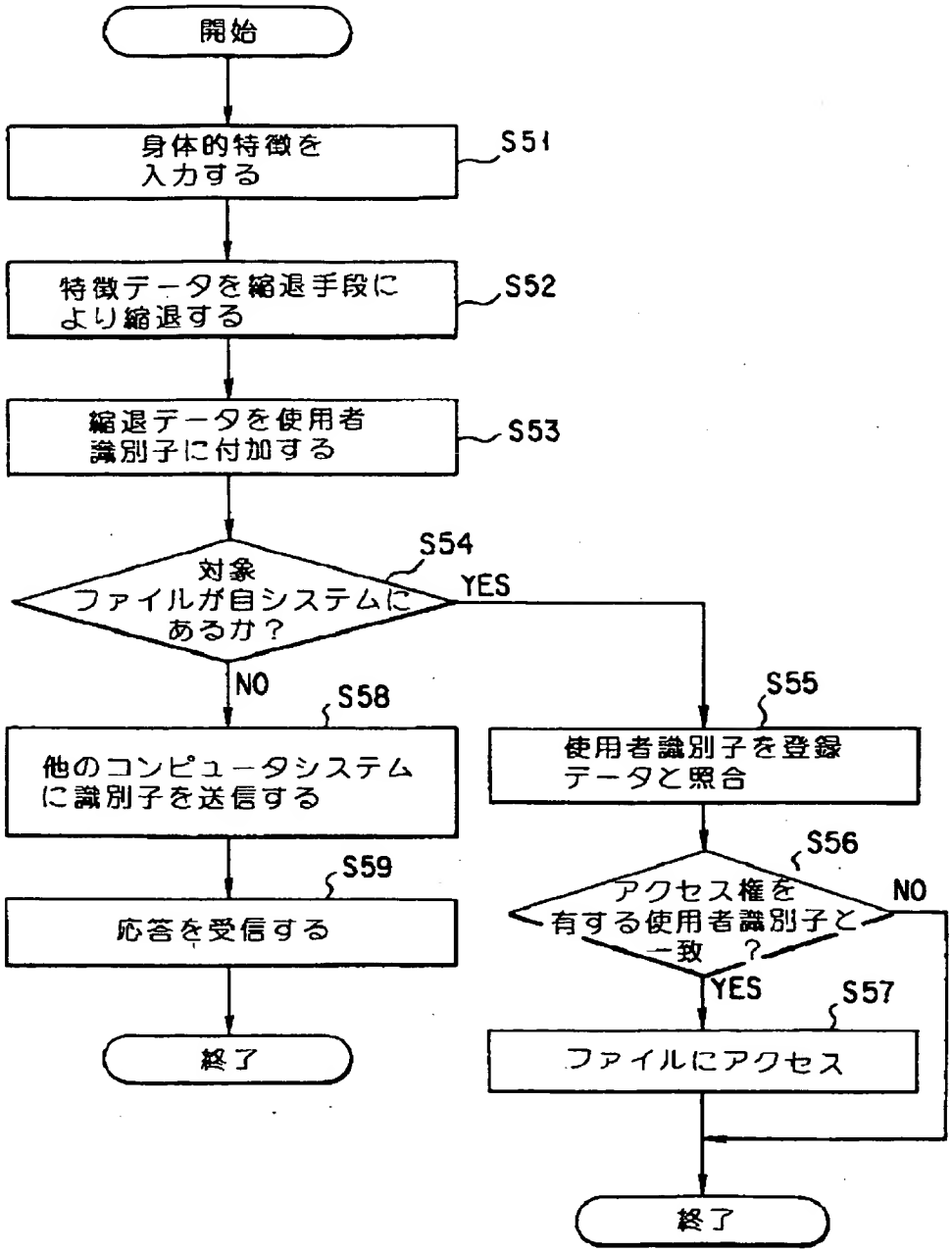
【図１０】


開始
S41
他のプロセスからの承認
手続き要求を受信
S42
指の特徴入力部により
特徴を入力
S43
承認
権利者としての
登録特徴と一致
？
NO
YES
S44
承認手続き処理実行
S45
次プロセスへ結果送信
終了

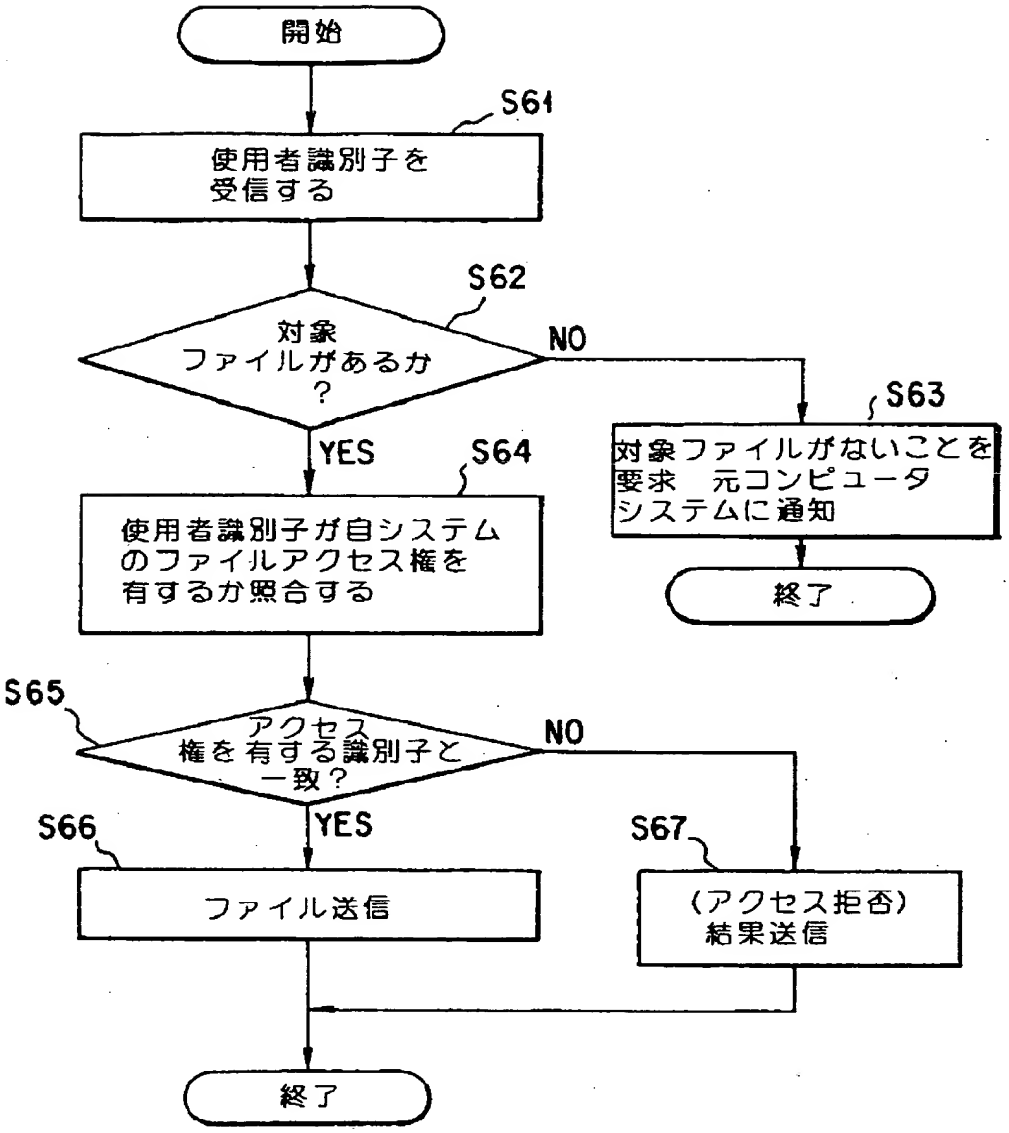
【図１１】


特徴計測ユニット
34-1
33-1
データ縮退
ユニット
30
31-1
コンピュータ
システム
35-1
特徴計測ユニット
34-2
データ縮退
ユニット
33-2
31-2
コンピュータ
システム
35-2
通信網
32
31-3
コンピュータ
システム
35-3
データ縮退
ユニット
33-3
特徴計測ユニット
34-3

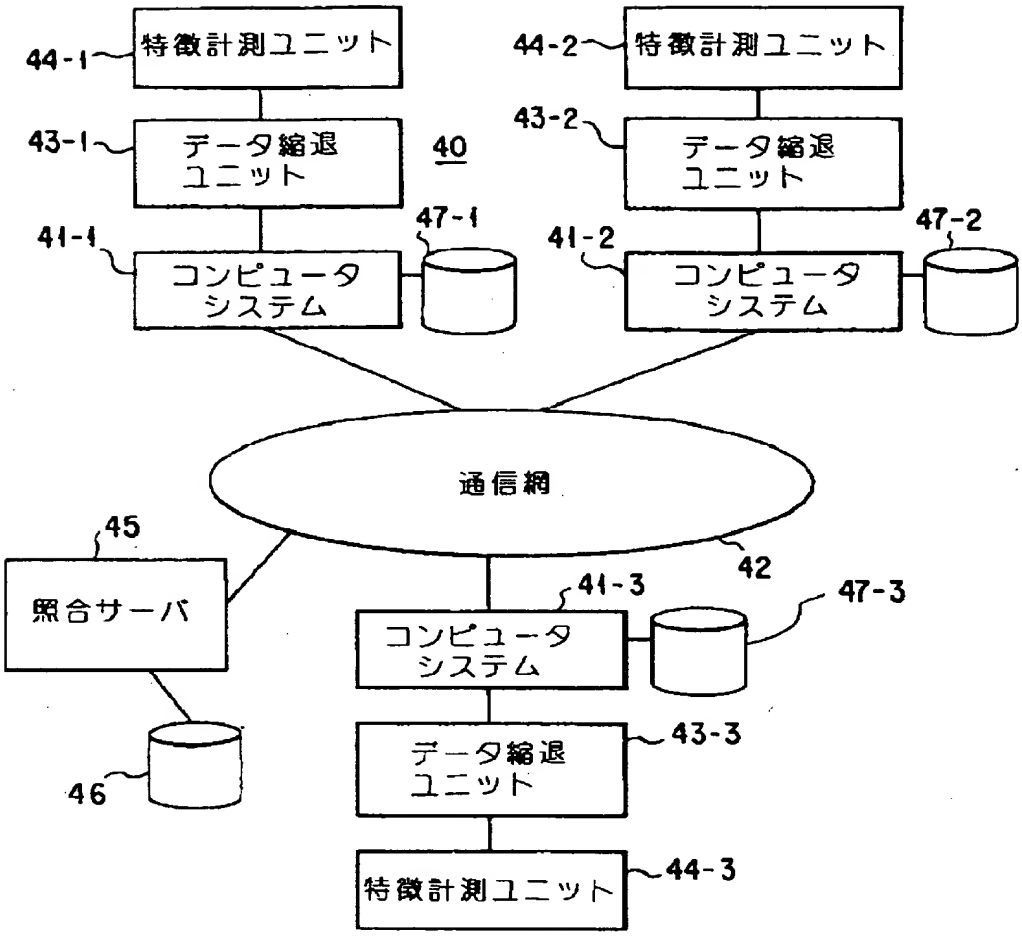
【図１２】


開始
身体的特徴を入力する
S51
特徴データを縮退手段により縮退する
S52
縮退データを使用者識別子に付加する
S53
対象ファイルが自システムにあるか？
S54
YES
NO
S58
他のコンピュータシステムに識別子を送信する
S59
応答を受信する
終了
S55
使用者識別子を登録データと照合
S56
アクセス権を有する使用者識別子と一致？
NO
YES
S57
ファイルにアクセス
終了

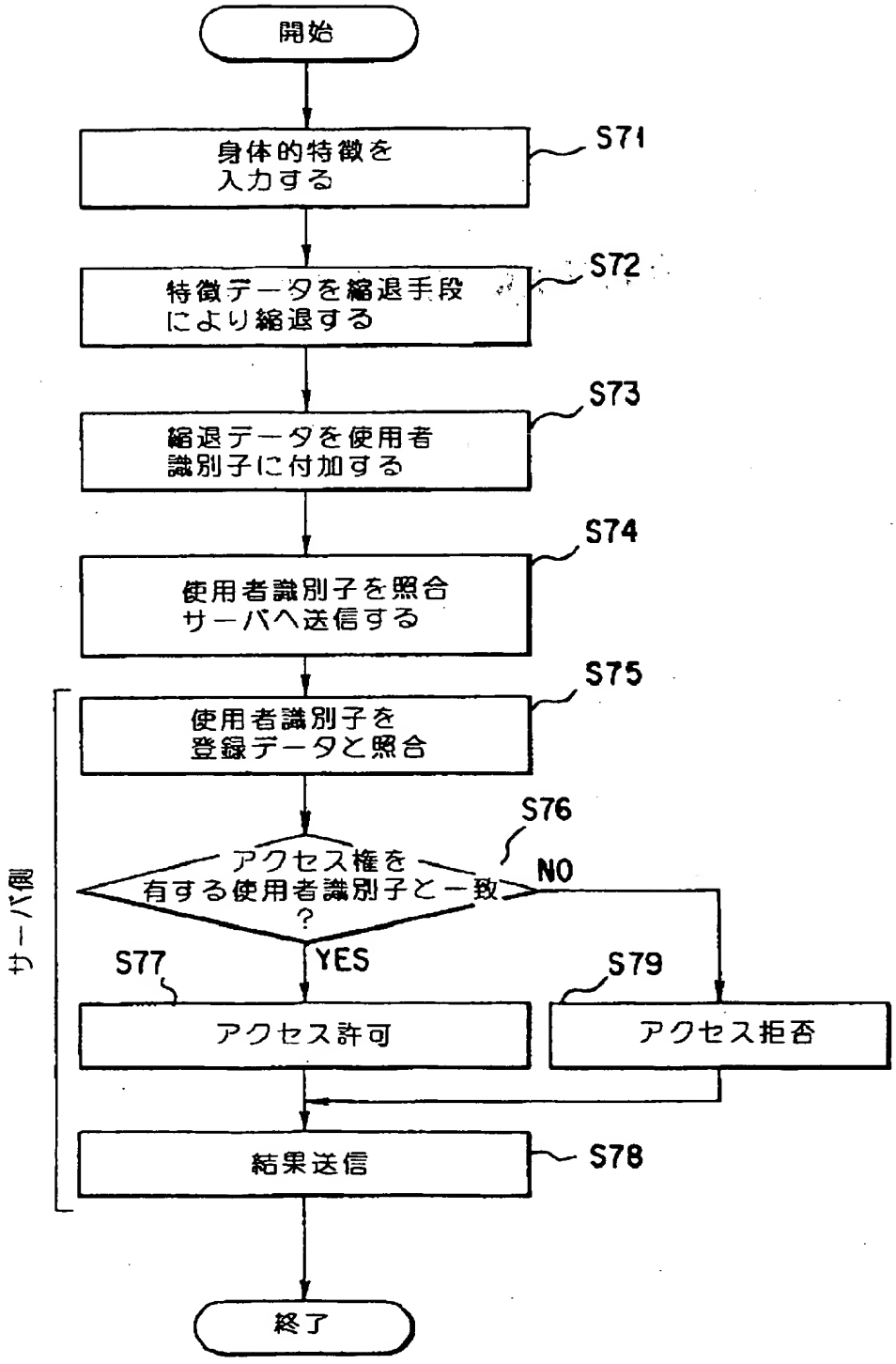
【図１３】


開始
S61
使用者識別子を
受信する
S62
対象
ファイルがあるか
？
NO
S63
対象ファイルがないことを
要求　元コンピュータ
システムに通知
終了
YES
S64
使用者識別子ガ自システム
のファイルアクセス権を
有するか照合する
S65
アクセス
権を有する識別子と
一致？
NO
YES
S66
ファイル送信
S67
（アクセス拒否）
結果送信
終了

【図１４】


44-1
特徴計測ユニット
44-2
特徴計測ユニット
43-1
データ縮退ユニット
40
43-2
データ縮退ユニット
41-1
コンピュータシステム
47-1
41-2
コンピュータシステム
47-2
通信網
45
照合サーバ
42
41-3
コンピュータシステム
47-3
43-3
データ縮退ユニット
46
44-3
特徴計測ユニット

【図１５】


開始
身体的特徴を入力する
S71
特徴データを縮退手段により縮退する
S72
縮退データを使用者識別子に付加する
S73
使用者識別子を照合サーバへ送信する
S74
使用者識別子を登録データと照合
S75
アクセス権を有する使用者識別子と一致？
S76
NO
YES
S77
アクセス許可
S79
アクセス拒否
結果送信
S78
終了
サーバ側